

~~DOCKET~~ FILE COPY ORIGINAL
Received & Inspected

APR -1 2009

FCC Mail Room

comspan
communications

March 26th, 2009

VIA FEDERAL EXPRESS

Federal Communications Commission
445 12th St S.W.
Washington, DC 20554

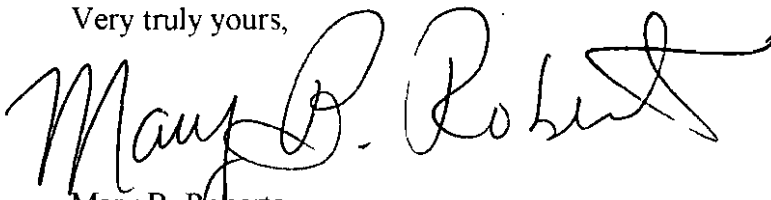
**Re: CC Docket No. 97-213: Policies and Procedures for Conducting Lawfully
Authorized Electronic Surveillance – ComSpan Communications Inc**

To Whom It May Concern:

Enclosed are an original and four updated copies of "ComSpan Communications Inc" manual setting forth the Company's policy and procedures for conducting lawfully authorized electronic surveillance, which we file pursuant to 47 CFR Section 64.2105 of the rules of the Federal Communications Commission ("The Commission"). This manual contains current company contacts and procedures.

Please acknowledge receipt of this filing by date stamping the extra copy of the Transmittal Letter and returning it in the enclosed, prepaid envelope. Inquiries pertaining to this filing should be directed to me at 541.229.4499.

Very truly yours,



Mary B. Roberts
Sr Manager of Customer Operations

Enclosures

No. of Copies rec'd 044
List ABCDE

Communications Assistance for
Law Enforcement Act
“CALEA”

Methods & Procedures

Table of Contents

BACKGROUND	4
INTRODUCTION	5
DEFINITIONS.....	6
POLICY STATEMENT	7
GENERAL POLICIES AND PROCEDURES FOR EMPLOYEES	7
DESIGNATED EMPLOYEES.....	8
PROCEDURES For the Conduct of Authorized surveillance	9
I. Call Content Interceptions <i>with</i> a Title III Court Order.....	9
II. Call Content Interceptions Pursuant to Title III but <i>without</i> a Court Order	10
III. Call Information Interceptions Using a Pen Register or Trap-and Trace Device <i>with</i> a Court Order	12
IV. Call Information Interceptions Using a Pen Register or Trap-and Trace Device <i>without</i> a Court Order	13
V. Electronic Surveillance <i>with</i> a Foreign Intelligence Surveillance Act (“FISA”) Court Order	14
VI. Electronic Surveillance Conducted Pursuant to FISA but <i>without</i> a Court Order	15
PROCEDURES IF UNAUTHORIZED SURVEILLANCE OR A COMPROMISE OF SURVEILLANCE HAS OCCURRED.....	16
COMMISSION REVIEW.....	17
APPENDIX A.....	18
DESIGNATED EMPLOYEES.....	18
APPENDIX B - LEGAL NOTIFICATION DOCUMENT	19
APPENDIX C – DETERMINATION RECORD.....	21
APPENDIX D – CERTIFICATION RECORD.....	23

EXHIBIT 1 – SAMPLE COURT ORDER FOR A PEN REGISTER OR TRAP AND TRACE DEVICE.....	25
--	----

US CODE: TITLE 50 > CHAPTER 36 > SUBCHAPTER I —ELECTRONIC SURVEILLANCE	27
---	----

BACKGROUND

The following are the COMSPAN COMMUNICATIONS (Company) policies and procedures implementing the Communications Assistance for Law Enforcement Act ("CALEA") to ensure access by law enforcement officials to facilities or equipment necessary for the interception of communications or access to call-identifying information.

Lawfully-authorized Electronic Surveillance (as that term is defined hereinafter) is a law enforcement tool that police and other authorized government agencies use to investigate and prosecute criminals. Its use by law enforcement agents is strictly limited by law. Lawfully-authorized Electronic Surveillance encompasses a law enforcement agency's or organization's collection of either (1) the content (any transfer of messages, signals, writing, images, sounds, data, or intelligence of any nature) of any communication sent by or to a subject of surveillance (often referred to as a "wiretap"); or (2) the dialing or signaling information that identifies the origin, direction, destination, or termination of any communication generated or received by a subject of surveillance by means of any equipment, facility, or service of a telecommunications carrier (this type of surveillance includes what is often referred to as Pen Registers and Trap and Trace Devices (as those terms are defined hereinafter).

In 1994 Congress passed CALEA. CALEA does not change or expand law enforcement's fundamental statutory authority to conduct various types of Electronic Surveillance. Instead, CALEA established (among other things) a requirement that telecommunications carriers establish and adhere to policies and procedures that require the affirmative intervention by and knowledge of their employees in effectuating any interception through their switching premises, and that such interception is done lawfully and documented carefully.

The following policies and procedures are consistent with the specific requirements found necessary by the Federal Communications Commission ("FCC" or "Commission"). Among other things, the following policies and procedures identify the Primary Designated Employee (as set forth on Appendix A attached hereto) of Company who is responsible for maintaining such security procedures. These policies and procedures also establish reporting and record-keeping requirements for informing law enforcement officials of all acts of unauthorized Electronic Surveillance that may occur on Company's premises, as well as any other compromises of the carriers' systems security and integrity procedures that involve the execution of Electronic Surveillance.

INTRODUCTION

The purpose of this manual is to make Company employees, including the Designated Employees, aware of Company's policies for CALEA systems security and integrity. These policies comply with CALEA, Section 229 of the Communications Act and the Commission's rules. The policies and procedures set forth herein are designed to ensure that our employees take only those actions authorized or required by applicable federal and state laws and regulations. CALEA requires common carriers to configure their systems and equipment in such a way that federal and state law enforcement agencies can perform traditional wiretapping functions despite rapidly changing technology. CALEA does not expand law enforcement's fundamental statutory authority to conduct Electronic Surveillance.

CALEA includes provisions designed to ensure that a carrier's employees act within the law, obtain only information that is authorized by law, and keep secure and accurate records of wiretapping activity. To implement CALEA the Federal Communications Commission ("Commission"), in CC Docket 97-213 released several Reports and Orders, which require common carriers to implement systems security policies and procedures for the supervision and control of its officers and employees responsible for implementing law enforcement wiretap requests. Failure to comply with these systems security policies and procedures may result in a forfeiture action by the Commission under Section 503(b) of the Communications Act.

This manual shall be maintained at the Company's corporate headquarters and at all switching centers of the Company. All employees are required to make themselves familiar with these policies and follow the procedures detailed herein. Designated Employees are also responsible for reviewing and becoming familiar with all the relevant state and federal statutes and regulations provisions relating to Electronic Surveillance. Designated Employees must sign an annual certification that they have carefully reviewed this manual. If an employee has any questions about any of the information contained herein, the employees should contact the Primary Designated Employee.

DEFINITIONS

In applying the policies and procedures detailed herein, the Company employees should use the following definitions:

Appropriate Legal Authorization means: (1) a court order signed by a judge or magistrate of competent jurisdiction authorizing or approving interception of wire or electronic communications; or (2) other authorization pursuant to 18 U.S. C. 2518(7), or any other relevant federal or state statute.

Appropriate Company Authorization means the policies and procedures adopted by the Company to authorize, direct, supervise and control officers and employees authorized to assist law enforcement in conducting any interception of communications or access to call-identifying information.

Appropriate Authorization means both Appropriate Legal Authorization and Appropriate Company Authorization both of which are required prior to taking any action. .

Company means ComSpan Communications.

Designated Employee are those employees authorized by Company to take reasonable actions to comply with valid law enforcement requests for Electronic Surveillance in accordance with the provisions of this manual.

Electronic Surveillance means the implementation of either the interception of the content of a call or the interception of information on the originating or terminating numbers of a call.

Pen Register is a device that identifies the numbers dialed or otherwise transmitted on the telephone line to which such device is attached.

Primary Designated Employee is a Designated Employee assigned by the Company with the responsibility for ensuring that Designated Employees of the Company are on call at all times to respond to requests for Electronic Surveillance from law enforcement agencies and for keeping law enforcement agencies informed of changes in Designated Employees and relevant information relating to contacting the Designated Employees. The Primary Designated Employee is also responsible for ensuring that all records required under the provisions of this manual are current and accurate.

Trap and Trace Device is a device that identifies the origination number of an instrument or device from which a wire or electronic communication is transmitted.

POLICY STATEMENT

This manual contains the policy and procedures of Company and the rights and responsibilities of all employees, including the Designated Employees, relating to Electronic Surveillance. It is the policy of Company to comply with all federal and state laws and regulations relating to Electronic Surveillance including CALEA. Thus, it is the policy of Company to ensure that any Electronic Surveillance or access to call-identifying information within its premises or facilities can be activated only in accordance with Appropriate Legal Authorization and Appropriate Company Authorization, as determined by an individual officer or employee of the Company pursuant to applicable federal and state statutes and regulations. It is also the policy of Company to comply with all

relevant record keeping requirements relating to Electronic Surveillance or access to call-identifying information.

Government agencies do not have the authority to remotely activate interceptions within the switching premises of a telecommunications carrier. Law enforcement personnel may not enter into the Company's property to conduct Electronic Surveillance without the Company's prior knowledge. If any employee becomes aware of any acts of unauthorized Electronic Surveillance on the Company's premises or any compromise or violation of authorized Electronic Surveillance or the policies and procedures contained herein, the employee is required to report the violation to the Primary Designated Employee as soon as possible. Information on the violation shall promptly be documented and a copy of the documentation forwarded by the Primary Designated Employee to the appropriate law enforcement agency.

GENERAL POLICIES AND PROCEDURES FOR EMPLOYEES

Company employees may permit only lawful, authorized Electronic Surveillance to be conducted on Company premises. No Company employee may take any action to initiate or participate in any Electronic Surveillance without Appropriate Authorization. Furthermore, regardless of the circumstances, an employee must always insist upon a written authorization.

No employee of the Company may disclose to any person other than relevant law enforcement officials and Designated Employees of the Company, the existence of any interception or surveillance. Employees are advised that discussion with any person other than law enforcement officials and Designated Employees with a need to know (including discussion with family or friends) is strictly prohibited. Unauthorized disclosure of such information constitutes a violation of this policy and a violation of federal and/or state law for which penalties (including immediate termination of employment) may be imposed.

There are several federal and state statutes under which law enforcement may request Electronic Surveillance. On the federal level these are: 1) Chapter 119 of Title 18 of the United States Code, entitled "Wire and Electronic Communications Interception and Interception of Oral Communications", which is the basic wiretapping statute; 2) Chapter 206 of Title 18, the Federal law relating to Pen Registers and Trap and Trace Devices and 3) Chapter 36 of Title 50 the United States Code, the statute relating to foreign intelligence and Electronic Surveillance. These federal statutes are attached at the end of this manual.

The procedures to be used vary slightly depending upon which statute has been invoked and whether a court order has been obtained. It is important that the Designated Employees follow the specific rules relating to the individual statutes. Certain Electronic Surveillance is authorized by statute without a court order due to special circumstances in which law enforcement has determined that an emergency situation exists (involving immediate danger of serious physical injury or death, national security or organized crime) and there is insufficient time to obtain a court order. This applies to either call content interception or call information interception using a Pen Register or Trap and Trace Device. In those circumstances, law enforcement officers may seek limited interception of communications absent a court order. However, the requesting law enforcement agency is required to seek court authorization within forty-eight (48) hours of the commencement of the Electronic Surveillance.

DESIGNATED EMPLOYEES

Company hereby designates the persons on Appendix A to serve as points of contact for law enforcement agencies. These persons shall be available to law enforcement agencies in such a manner that law enforcement agencies will always be able to contact at least one of them 24 hours a day, 7 days a week. Company shall comply by providing the relevant positions and offices, and Central Contact Numbers, which are available 24 hours per day 7 days per week, as set forth on Appendix A. The Central =Contact Numbers are answered/monitored by Company staff, who provide support and supervision for Company's network on a 24/7 basis and which includes an out of hours emergency voice-mail box that is managed at all times. Company will supply the Central Contact Number staff at all times with current telephone numbers, cell phone numbers, and pager numbers for the following positions, at least one of which is to be available at all times to receive and respond to requests for services from law enforcement agencies. Law enforcement agencies seeking such services may obtain these services and contact all persons listed below through the following options:

1. 1-866-535-9858 M-F 24X7 Live Answer.
2. Contact personnel through information listed on Appendix A which includes escalation contacts.

The contact persons and numbers are provided on Appendix A for immediate out of hours contact and redundancy. These numbers will not necessarily be available 24 hours per day, seven days per week, but will serve as additional and backup numbers, including a successive escalation order.

Company shall provide the requesting law enforcement agency by facsimile transmission or in electronic form, the form attached as Appendix B, which shall be completed and faxed to Company with appropriate identification and authorization by court order or emergency request before any surveillance service is initiated, to ensure that unauthorized surveillance does not occur.

PROCEDURES For the Conduct of Authorized Surveillance

I. Call Content Interceptions *with* a Title III Court Order

- Step One: Any court order presented by a law enforcement agency for a call content interception pursuant to Title III shall be referred immediately to one of the Designated Employees. The law enforcement agency representative shall complete and sign the Legal Notification Document which appears as Appendix B, and shall provide proper identification. The Designated Employee shall immediately inform the Company Legal Department or CEO
- Step Two: Before implementing the interception, the Designated Employee shall ensure that the court order contains the following information:
- (a) the identity of the person, if known, whose communications are to be intercepted;
 - (b) The nature and location of the communication facilities or the place for which authority to intercept is granted;
 - (c) A particular description of the type of communication sought to be intercepted and a statement of the particular offense to which it relates;
 - (d) The period of time during which the interception is authorized, including a statement whether the interception shall automatically terminate when the described communication has been first obtained;
 - (e) A provision that the authorization to intercept shall be executed as soon as practicable and conducted in such a way as to minimize the interception of communications not otherwise subject to interception; **AND**
 - (f) The signature of a judge or magistrate.
- [A sample court order for a pen register or trap-and trace device is attached as Exhibit 1]**
- Step Three: The designated Employee also shall determine whether the surveillance can be implemented technically **AND** whether the court order is sufficiently and accurately detailed to enable the carrier to comply with its terms. If the request cannot be implement, the Designated Employee will need to complete a Determination Record (attached hereto as Appendix C), and notify the requesting law enforcement agency as to the reason. In those instances where the Company's underlying carrier will need to perform the Electronic Surveillance, the Company will provide the name of the underlying carrier to the requesting law enforcement agency.
- Step Four: The Designated Employee may implement the surveillance and may delegate tasks associated with the surveillance to other employees, but the Designated Employee shall continue to oversee the implementation of the surveillance.
- Step Five: The Designated Employee shall complete a Certification Form (attached as Appendix D) as soon as possible after the initiation of the Electronic Surveillance. The employee shall supply all information requested on the Certification Form that is not contained on the court order. The employee then shall attach the court order to the Certificate Form and sign the Certification Form. The employee also shall attach to the Certification Form any extensions that are granted for the surveillance.

- Step Six The Designated Employee shall ensure that the Certification Form and all attachments are placed in the appropriate file.
- Step Seven The Designated Employee shall continue to oversee the conduct of the Electronic Surveillance and ensure that the surveillance terminates at the time specified in the court order (which, in the absence of an extension, cannot exceed 30 days)

II. Call Content Interceptions Pursuant to Title III but *without* a Court Order

- Step One: Any request by a law enforcement agency for a call content interception without a court order, pursuant to the exigent circumstances listed in 18 U.S.C. 2518(7), shall be referred immediately to one of the Designated Employees. The law enforcement agency representative shall complete and sign the Legal Notification Document which appears as Appendix B, and shall provide proper identification. The Designated Employee shall immediately inform the Company Legal Department or CEO.
- Step Two: Before implementing the interception, the Designated Employee shall ensure that the law enforcement agency provides a certification containing the following information:
- (a) the information, facilities, or technical assistance required;
 - (b) the period of time during which the provision of information, facilities, or technical assistance is authorized;
 - (c) a statement that no warrant or court order is required by law;
 - (d) a statement that all statutory requirements have been met;
 - (e) a statement that the specific requested assistance is required; **AND**
 - (f) the signature of **EITHER** (i) the Attorney General of the United States, **OR** (ii) a law enforcement officer specially designated by the Attorney General, the Deputy Attorney General, the Associate Attorney General, or by the principal prosecuting attorney of any state or subdivision thereof.
- Step Three: The Designated Employee also shall determine whether the surveillance can be implemented technically **AND** whether the certification is sufficiently and accurately detailed to enable the carrier to comply with its terms. If the request cannot be implemented, the Designated Employee will need to complete a Determination Record (attached hereto as Appendix C), and notify the requesting law enforcement agency as to the reason. In those instances where the Company's underlying carrier will need to perform the Electronic Surveillance, the Company will provide the name of the underlying carrier to the requesting law enforcement agency.
- Step Four: The Designated Employee may implement the surveillance and may delegate tasks associated with the surveillance to other employees, but the Designated Employee shall continue to oversee the implementation of the surveillance.
- Step Five: The Designated Employee shall complete a Certification Form (attached as Appendix D) as soon as possible after the initiation of the Electronic Surveillance. The employee shall supply all information requested on the Certification Form that is not contained on the certification provided by the law enforcement agency and sign the Certification Form.
- Step Six: The Designated Employee shall ensure that the Certification Form and all attachments are placed in the appropriate file
- Step Seven: The Designated Employee shall continue to oversee the conduct of the Electronic Surveillance and terminate the surveillance as soon as any of the following events occur:
- I. the law enforcement agency does not apply for a court order within 48 hours after the interception has begun; or
 - II. the law enforcement agency's application for a court order is denied.
- Step Eight: If the law enforcement agency receives a court order for the surveillance, the Designated Employee shall validate the court order (as specified in Section I, Step Two above),

attach the order to the Certification Form, and handle the surveillance in all respects under the procedures in Section I above.

III. Call Information Interceptions Using a Pen Register or Trap and Trace Device *with* a Court Order

- Step One:** Any court order presented by a law enforcement agency for a call information interception using a pen register or trap-and-trace device shall be referred immediately to one of the Designated Employees. The law enforcement agency representative shall complete and sign the Legal Notification Document which appears as Appendix B, and shall provide proper identification. The Designated Employee shall immediately inform the Company Legal Department or CEO.
- Step Two:** Before implementing the interception, the Designated Employee shall determine that the court order contains the following information:
- (a) the identity, if known, of the person to whom is leased or in whose name is listed the telephone line to which the pen register or trap and trace device is to be attached;
 - (b) the identity, if known, of the person who is the subject of the criminal investigation;
 - (c) the number and, if known, physical location of the telephone line to which the pen register or trap and trace device is to be attached and, in the case of a trap-and-trace device, the geographical limits of the trap-and-trace order;
 - (d) a statement of the offense to which the information likely to be obtained by the pen register or trap-and-trace device relates: **AND**
 - (e) the signature of a judge or magistrate

[A sample court order for a pen register or trap-and trace device is attached as Exhibit 1]

- Step Three:** The Designated Employee also shall determine whether the surveillance can be implemented technically **AND** whether the court order is sufficiently and accurately detailed to enable the carrier to comply with its terms. If the request cannot be implemented, the Designated Employee will need to complete a Determination Record (attached hereto as Appendix C), and notify the requesting law enforcement agency as to the reason. In those instances where the Company's underlying carrier will need to perform the Electronic Surveillance the company will provide the name of the underlying carrier to the requesting law enforcement agency
- Step Four:** The Designated Employee may implement the surveillance and may delegate tasks associated with the surveillance to other employees, but the Designated Employee shall continue to oversee the implementation of the surveillance.
- Step Five:** The Designated Employee shall complete a Certification Form (attached as Appendix D) as soon as possible after the initiation of the Electronic Surveillance. The employee shall supply all information requested on the Certification Form that is not contained on the court order. The employee then shall attach the court order and sign the Certification Form. The employee also shall attach any extensions that are granted for the surveillance.
- Step Six:** The Designated Employee shall ensure that the Certification Form and all attachments are placed in the appropriate file.
- Step Seven:** The Designated Employee shall continue to oversee the conduct of the Electronic Surveillance and ensure that the surveillance terminates when the legal authorization expires. The Designated Employee shall terminate the surveillance at the time specified in the order (which, in the absence of an extension, cannot exceed 60 days).

IV. Call Information Interceptions Using a Pen Register or Trap-and Trace Device *without* a Court Order

- Step One:** Any request for a call information interception using a pen register or trap-and-trace device without a court order shall be referred immediately to one of the Designated Employees. The law enforcement agency representative shall complete and sign Legal Notification Document which appears as Appendix B, and shall provide proper identification. The Designated Employee shall immediately inform the Company Legal Department.
- Step Two:** Although the federal statute does not expressly require a certification in these circumstances, the Designated Employee shall ensure that the law enforcement agency provides a certification containing the following information before implementing the request:
- (a) the information, facilities or technical assistance required;
 - (b) the period of time during which the provision of information, facilities, or technical assistance is authorized;
 - (c) a statement that no warrant or court is required by law;
 - (d) a statement that all statutory requirements have been met;
 - (e) a statement that the specific requested assistance is required; **AND**
 - (f) the signature of a law enforcement officer specially designated by the Attorney General of the United States, the Deputy Attorney General, the Associate Attorney General, and Assistant Attorney General, or by the principal prosecuting attorney of any state or subdivision thereof.
- Step Three:** The Designated Employee also shall determine whether the surveillance can be implemented technically **AND** whether the certification is sufficiently and accurately detailed to enable the carrier to comply with its terms. If the request cannot be implemented, the Designated Employee will need to complete a Determination Record (attached hereto as Appendix C), and notify the requesting law enforcement agency as to the reason. In those instances where the Company's underlying carrier will need to perform the Electronic Surveillance the Company will provide the name of the underlying carrier to the requesting law enforcement agency.
- Step Four:** The Designated Employee may implement the surveillance and may delegate tasks associated with the surveillance to other employees, but the Designated Employee shall continue to oversee the implementation of the surveillance.
- Step Five:** The Designated Employee shall complete a Certification Form (attached as Appendix D) as soon as possible after the initiation of the Electronic Surveillance. The employee shall supply all information requested on the Certification Form that is not contained on the certification provided by the law enforcement agency. The employee then shall attach the certification provided by the law enforcement agency and sign the Certification Form.
- Step Six:** The Designated Employee shall ensure that the Certification Form and all attachments are placed in the appropriate file
- Step Seven:** The Designated Employee shall continue to oversee the conduct of the Electronic Surveillance and terminate the surveillance as soon as any of the following events occur:
- (a) the information sought is obtained;
 - (b) the law enforcement agency's application for the court order is denied; or
 - (c) 48 hours have lapsed since the installation of the device without the granting of a court order
- Step Eight:** If the law enforcement agency does not receive a court order for the surveillance, the Designated Employee shall validate the court order (as specified in Section I, Step Two

above), attach the order to the Certification Form, and handle the surveillance in all respects under the procedures in Section I above.

V. Electronic Surveillance *with* a Foreign Intelligence Surveillance Act ("FISA") Court Order

Step One: Any court order presented by a law enforcement agency for Electronic Surveillance pursuant to FISA shall be referred immediately to one of the Designated Employees designated on Appendix A of this manual. The law enforcement agency representative shall complete and sign the Legal Notification Document which appears as Appendix B, and shall provide proper identification. The Designated Employee shall immediately inform the Company Legal Department or CEO.

Step two: Before implementing the interception, the Designated Employee shall ensure that the court order contains the following information:

- (a) The identity, if known, or a description of the target of the Electronic Surveillance;
- (b) The nature and location of each of the facilities or places at which the Electronic Surveillance will be directed;
- (c) The type of information sought to be acquired and the type of communications or activities to be subjected to the surveillance;
- (d) The means by which the Electronic Surveillance will be effected and whether physical entry will be used to effect the surveillance;
- (e) The period of time during which the Electronic Surveillance is approved;
- (f) Whenever more than one electronic, mechanical, or other surveillance device is to be used under the order, the authorized coverage of the devices involved and what minimization procedures shall apply to information subject to acquisition by each device;
- (g) A statement directing that the minimization procedures be followed;
- (h) A statement directing that, upon the request of the applicant, a specified carrier furnish the applicant forthwith all information, facilities, or technical assistance necessary to accomplish the Electronic Surveillance in such a manner as will protect its secrecy and produce a minimum of interference with the services that the carrier is providing that target of Electronic Surveillance;
- (i) A statement directing that the carrier maintain under security procedures approved by the attorney General and the Director of Central Intelligence any record concerning the surveillance or the aid furnished that such person wishes to retain;
- (j) A statement directing that the applicant compensate, at the prevailing rate, the carrier for furnishing the aid; **AND**
- (k) The signature of a federal district judge.

Whenever the target of the Electronic Surveillance is a foreign power (as defined under FISA) and each of the facilities or places at which the surveillance is directed is owned, leased, or exclusively used by that foreign power, the court order need not contain the information required by subparagraphs (c), (d), and (f), but shall generally describe the information sought, the communications or activities to be subjected to the surveillance, and the type of Electronic Surveillance involved, including whether physical entry is required.

Step Three: The Designated Employee also shall determine whether the surveillance can be implemented technically **AND** whether the court order is sufficiently and accurately detailed to enable the carrier to comply with its terms. If the request cannot be implemented, the Designated Employee will need to complete a Determination Record

(attached hereto as Appendix C), and notify the requesting law enforcement agency as to the reason. In those instances where the Company's underlying carrier will need to perform the Electronic Surveillance, the Company will provide the name of the underlying carrier to the requesting law enforcement agency.

Step Four: The Designated Employee may implement the surveillance and may delegate the tasks associated with the surveillance to other employees, but the Designated Employee shall continue to oversee the implementation of the surveillance.

Step Five: The Designated Employee shall complete a Certification Form (attached as Appendix D) as soon as possible after the initiation of the Electronic Surveillance. The employee shall supply all information requested on the Certification Form that is not contained on the court order. The employee then shall attach the court order and sign the Certification Form. The employee also shall attach any extensions that are granted for the Surveillance.

Step Six: The Designated Employee shall ensure that the Certification Form and all attachments are placed in the appropriate file.

Step Seven: The Designated Employee shall continue to oversee the conduct of the Electronic Surveillance and ensure that the surveillance terminates when the legal authorization expires. The interception shall be terminated at the time specified in the order. In the absence of an extension, the surveillance cannot exceed 90 days (or 1 year if the surveillance is targeted against a foreign power).

VI. Electronic Surveillance Conducted Pursuant to FISA but *without* a Court Order

Step One: Any request by a law enforcement agency for Electronic Surveillance pursuant to FISA but without a court order shall be referred immediately to one of the Designated Employees on Appendix A. The law enforcement agency representative shall complete and sign the Legal Notification Document which appears as Appendix B, and shall provide proper identification. The Designated Employee shall immediately inform the Company Legal Department.

Step Two: Although FISA does not expressly require a certification in these circumstances, the Designated Employee shall ensure that the law enforcement agency provides a certification containing the following information before implementing the request.

- (a) the information, facilities, or technical assistance required;
- (b) the period of time during which the providing of information, facilities, or technical assistance is authorized;
- (c) a statement that no warrant or court order is required by law;
- (d) a statement that all statutory requirement have been met;
- (e) a statement that the specific requested assistance is required; **AND**
- (f) the signature of **Either** (i) the Attorney General of the United States, **OR** (ii) a law enforcement officer specially designated by the Attorney General.

Step Three: The Designated Employee also shall determine whether the surveillance can be implemented technically **AND** whether the certification is sufficiently and accurately detailed to enable the carrier to comply with its terms. If the request cannot be implement, the Designated Employee will need to complete a Determination Record (attached hereto as Appendix C), and notify the requesting law enforcement agency as to the reason. In those instances where the Company's underlying carrier will need to perform the Electronic Surveillance, the Company will provide the name of the underlying carrier to the requesting law enforcement agency.

- Step Four: The Designated Employee may implement the surveillance and may delegate tasks associated with the surveillance to other employees, but the Designated Employee shall continue to oversee the implementation of the surveillance.
- Step Five: The Designated Employee shall complete a Certification Form (attached as Appendix D) as soon as possible after the initiation of the Electronic Surveillance. The employee shall supply all information requested on the Certification Form that is not contained on the certification provided by the law enforcement agency. The employee then shall attach the certification provided by the law enforcement agency and sign the Certification Form.
- Step Six: The Designated Employee shall ensure that the Certification Form and all Attachments are placed in the appropriate file.
- Step Seven: The designated Employee shall continue to oversee the conduct of the Electronic Surveillance and terminate the surveillance as soon as any of the following events occur:
- (a) the information sought is obtained;
 - (b) the law enforcement agency's application for a court order is denied; or
 - (c) 24 hours have elapsed since the authorization of the surveillance by the Attorney General without the granting of a court order.
- Step Eight: If the law enforcement agency does receive a court order for the surveillance, the Designated Employee shall validate the court order (as specified in Section I, Step Two above), attach the order to the Certification Form, and handle the surveillance in all respects under the procedures in Section I above.

PROCEDURES IF UNAUTHORIZED SURVEILLANCE OR A COMPROMISE OF SURVEILLANCE HAS OCCURRED

- Step One: If any employee becomes aware of any act of unauthorized Electronic Surveillance or any compromise of authorized surveillance to unauthorized persons or entities, that employee shall report the incident immediately to one of the Designated Employees in Appendix A. The law enforcement agency representative shall complete and sign the Legal Notification Document which appears as Appendix B, and shall provide proper identification.
- Step Two: The Designated Employee shall promptly notify Chris McLorg President, and the Company legal department of the incident. Acting with the President and legal counsel, the Designated Employee and Chris McLorg or (legal counsel) shall determine which law enforcement agencies are affected and promptly notify the agencies of the incident.
- Step Three: The Designated Employee shall compile a certification record for any unauthorized surveillance and ensure that all record available to the carrier regarding the surveillance are placed in the appropriate carrier files. If the request cannot be implemented, the Designated Employee will need to complete a Determination Record (attached hereto as Appendix C), and notify the requesting law enforcement agency as to the reason. In those instances where the Company's underlying carrier will need to perform the Electronic Surveillance, the Company will provide the name of the underlying carrier to the requesting law enforcement agency.

COMMISSION REVIEW

The Company shall file these policies and procedures with the Commission within ninety (90) days of the Company's merger or divestiture or the Company's amendment of its existing policy and procedures.

APPENDIX A

DESIGNATED EMPLOYEES

Primary Designated Employee	Brian Medley	GM Operations	541-229-2154, 425-941-6210
------------------------------------	--------------	---------------	-------------------------------

Service Site	Name	Position	Telephone Number(s) (Office, Cell, Home)
Roseburg OR	Mary Roberts M-F 8am-5pm only	SR Manager of Service Operations	541-229-4499, 541 390 0190
Roseburg OR	Cliff Farley	Switch Engineer	541-229-0222, 541-643-9208
Roseburg OR	Aaron Blakely	IP Engineer	541-430-5805
Roseburg OR	Tim Spanning	Operations Manager	360-989-0448

APPENDIX B - LEGAL NOTIFICATION DOCUMENT

PEN REGISTER, TRAP AND TRACE DEVICE, AND WIRE COMMUNICATIONS INTERCEPTION

LEGAL NOTIFICATION DOCUMENT

A copy of Requestor's identification MUST be attached to this form before commencing Services.

SERVICE TYPE	
<i>Please check all applicable boxes:</i>	
<input type="checkbox"/> Pen Register	<input type="checkbox"/> Emergency Service <input type="checkbox"/> Non-Emergency Service
<input type="checkbox"/> Trap and Trace Device	<input type="checkbox"/> Emergency Service <input type="checkbox"/> Non-Emergency Service
<input type="checkbox"/> Wire Communications Interception	<input type="checkbox"/> Emergency Service <input type="checkbox"/> Non Emergency Service
<input type="checkbox"/> Court Order	<input type="checkbox"/> Other [Please Specify] _____

Retain a copy of the document and attach the original to this form.

Commencement Date: _____ Termination Date:* _____

** As specified in the court document, or in the absence thereof, Authorized Requestor's estimated time frame*

Authorized Requestor (printed name)

Authorized Requestor (Signature)

Date

Agency Name

() _____
Phone Number

Superior Name No. 1

() _____
Phone Number

Superior Name No. 2

() _____
Phone Number

Provider (printed name)

Provider (Signature)

INSTRUCTIONS:

APPENDIX C – DETERMINATION RECORD

The undersigned, an employee designated by the Company to respond to and oversee the implementation of legal Electronic Surveillance requests from law enforcement agencies hereby certifies that the Company cannot implement the requested Electronic Surveillance for the reason(s) noted below.

A. Telephone number(s) and/or circuit identification numbers involved:

B. Requested start date (including date and time):

C. Name of person signing the Appropriate Legal Authorization:

D. The type of interception of communications or access to call-identifying information (e.g., Pen Register, Trap and Trace Device)

E. Reason that the interception of communications or access to call-identifying information cannot technically be provided (e.g., technical inability; customer of a different carrier)

F. Name of the Company's personnel responsible for overseeing the interception of communication or access to call-identifying information and signing this form:

Signature

()
Phone Number

APPENDIX D – CERTIFICATION RECORD

The undersigned, Designated Employee, hereby certifies that this is a true and complete record of the information received and actions taken relative to the attached Appropriate Legal Authorization. The undersigned further certifies that on the date and time indicated below, appropriate actions were taken to implement the Electronic Surveillance referenced in the attached court order or Certification relating to the following:

A. Telephone number(s) and/or circuit identification numbers involved:

B. Start date (including date and time) of the circuit opening for law enforcement:

C. Name of person signing the Appropriate Legal Authorization:

D. The type of interception of communications or access to call-identifying information:

E. The date that the interception is scheduled to be terminated and actual date terminated.

Scheduled

Extension

Actual Termination

F. Name of the Company's personnel responsible for overseeing the interception of communication or access to call-identifying information and signing this form:

Printed Name

Signature

Date

EXHIBIT 1 – SAMPLE COURT ORDER FOR A PEN REGISTER OR TRAP AND TRACE DEVICE

The following is an example only of a Court Order Submitted by a Law Enforcement Agency for a Call Information Interception

IN THE MATTER OF THE APPLICATION
BY [JURISDICTION] FOR AN ORDER
AUTHORIZING THE INSTALLATION AND
USE OF A PEN REGISTER AND/OR
TRAP AND TRACE

ORDER

This matter having come before the court pursuant to an application under title 18, United States Code, Section 3122 by [Name], an attorney for the Government, which application requests an order under Title 18, United States Code, Section 3122 authorizing the installation and use of a pen register and/or trap and trace on [telephone number(s)], the court finds that the applicant has certified that the information likely to be obtained by such installation and use is relevant to an ongoing investigation into possible violations of [Specific Criminal Offense(s)] by [Person(s)], and located at [address], is/are relevant to an ongoing criminal investigation of the specified offenses,

IT APPEARING that the numbers dialed or pulsed from/to [telephone number(s)], listed to or leased by [name(s) of person(s)], located at [address], is/are relevant to an ongoing criminal investigation of the specified offenses,

IT IS ORDERED, pursuant to Title 18, United States Code, Sections 3123 and 3124, that agents of [Investigative Agency] may install and use a pen register and/or trap and trace to register numbers dialed or pulsed from or to [telephone number(s)], to record the date and time of such pulsing or recordings, and to record the length of time the telephone receiver(s) in question is/are off the hook for incoming or outgoing calls for a period of [Not to Exceed 60 Days], and if trap and trace order, [geographic limitations]; and,

IT IS FURTHER ORDERED, pursuant to Title 18, United States Code, Section 3124, that [Carrier] shall furnish agents of the [Investigative Agency] forthwith all information, facilities and technical assistance necessary to accomplish the installation of the pen register and/or trap and trace unobtrusively and with minimum interference to the services that are accorded persons with respect to whom the installation and use is to take place; and

IT IS FURTHER ORDERED, that [Carrier] be compensated by the applicant for reasonable expenses incurred in providing technical assistance; and

IT IS FURTHER ORDERED, that [Carrier] shall supply [Investigative Agency] with subscriber information, including published and nonpublished telephone information, for those telephone numbers, names or addresses identified in this order and/or obtained by the pen register and/or trap trace installed pursuant to this order; and

IT IS FURTHER ORDERED, pursuant to Title 18, United States Code, Section 3123, that this order and the application be sealed until otherwise ordered by the Court, and that [Carrier], its agents and employees shall not disclose the existence of the pen register and/or trap and trace, or the existence of the investigation to the listed subscriber, or to any other person, unless or until otherwise ordered by the court.

JUDGE

DATE

NOTE: The above is a sample of a basis court order for a pen register or trap/trace. In addition to the above, the court order is to include other specifics required by law enforcement. A carrier cannot provide information that is not specified and required by court order. Title III Wire Intercepts follow the same basic format; however, the time frame cannot exceed 30 days.

US CODE: TITLE 50 > CHAPTER 36 > SUBCHAPTER I — ELECTRONIC SURVEILLANCE

§ 1807. Report to Administrative Office of the United States Court and to Congress

In April of each year, the Attorney General shall transmit to the Administrative Office of the United States Court and to Congress a report setting forth with respect to the preceding calendar year—

- (a) the total number of applications made for orders and extensions of orders approving electronic surveillance under this subchapter; and
- (b) the total number of such orders and extensions either granted, modified, or denied.

§ 1808. Report of Attorney General to Congressional committees; limitation on authority or responsibility of information gathering activities of Congressional committees; report of Congressional committees to Congress

Report of Attorney General to Congressional committees; limitation on authority or responsibility of information gathering activities of Congressional committees; report of Congressional committees to Congress

(a) (1) On a semiannual basis the Attorney General shall fully inform the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence concerning all electronic surveillance under this subchapter. Nothing in this subchapter shall be deemed to limit the authority and responsibility of the appropriate committees of each House of Congress to obtain such information as they may need to carry out their respective functions and duties.

(2) Each report under the first sentence of paragraph (1) shall include a description of—
(A) each criminal case in which information acquired under this chapter has been passed for law enforcement purposes during the period covered by such report; and
(B) each criminal case in which information acquired under this chapter has been authorized for use at trial during such reporting period.

(b) On or before one year after October 25, 1978, and on the same day each year for four years thereafter, the Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence shall report respectively to the House of Representatives and the Senate, concerning the implementation of this chapter. Said reports shall include but not be limited to an analysis and recommendations concerning whether this chapter should be

- (1) amended,
- (2) repealed, or
- (3) permitted to continue in effect without amendment.

§ 1809. Criminal sanctions

(a) Prohibited activities

A person is guilty of an offense if he intentionally—

- (1) engages in electronic surveillance under color of law except as authorized by statute; or
- (2) discloses or uses information obtained under color of law by electronic surveillance, knowing or having reason to know that the information was obtained through electronic surveillance not authorized by statute.

(b) Defense

It is a defense to a prosecution under subsection (a) of this section that the defendant was a law enforcement or investigative officer engaged in the course of his official duties and the electronic surveillance was authorized by and conducted pursuant to a search warrant or court order of a court of competent jurisdiction.

(c) Penalties

An offense described in this section is punishable by a fine of not more than \$10,000 or imprisonment for not more than five years, or both.

(d) Federal jurisdiction

There is Federal jurisdiction over an offense under this section if the person committing the offense was an officer or employee of the United States at the time the offense was committed.

§ 1810. Civil liability

An aggrieved person, other than a foreign power or an agent of a foreign power, as defined in section 1801 (a) or (b)(1)(A) of this title, respectively, who has been subjected to an electronic surveillance or about whom information obtained by electronic surveillance of such person has been disclosed or used in violation of section 1809 of this title shall have a cause of action against any person who committed such violation and shall be entitled to recover—

- (a) actual damages, but not less than liquidated damages of \$1,000 or \$100 per day for each day of violation, whichever is greater;
- (b) punitive damages; and
- (c) reasonable attorney's fees and other investigation and litigation costs reasonably incurred.

§ 1811. Authorization during time of war

Notwithstanding any other law, the President, through the Attorney General, may authorize electronic surveillance without a court order under this subchapter to acquire foreign intelligence information for a period not to exceed fifteen calendar days following a declaration of war by the Congress.

§ 1821. As used in this subchapter:

- (1) The terms "foreign power", "agent of a foreign power", "international terrorism", "sabotage", "foreign intelligence information", "Attorney General", "United States person", "United States", "person", and "State" shall have the same meanings as in section 1801 of this title, except as specifically provided by this subchapter.